



## Bescheinigung

Die Francotyp-Postalia AG & Co in Birkenwerder/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren zum Schutz eines Sicherheitsmoduls und  
Anordnung zur Durchführung des Verfahrens"

am 12. März 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig das Symbol G 11 C 5/14 der Internationalen Patentklassifikation erhalten.

München, den 14. Februar 2000

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Holt

Zeichen: 199 12 781.6

CERTIFIED COPY OF  
PRIORITY DOCUMENT

Francotyp-Postalia AG & Co.  
Triftweg 21 - 26  
16547 Birkenwerder

12. März 1999

3149-DE

---

Verfahren zum Schutz eines Sicherheitsmoduls und Anordnung zur  
Durchführung des Verfahrens

---

Beschreibung

Die Erfindung betrifft ein Verfahren zum Schutz eines Sicherheitsmoduls, gemäß der im Oberbegriff des Anspruchs 1 angegebenen Art, und eine Anordnung zur Durchführung des Verfahrens, gemäß der im Oberbegriff des Anspruchs 3 angegebenen Art. Ein solcher postalischer Sicherheitsmodul ist insbesondere für den Einsatz in einer Frankiermaschine bzw. Postbearbeitungsmaschine oder Computer mit Postbearbeitungsfunktion geeignet.

Moderne Frankiermaschinen, wie die aus der US 4.746.234 bekannte Thermotransfer-Frankiermaschine, setzen eine vollelektronische digitale Druckvorrichtung ein. Damit ist es prinzipiell möglich, beliebige Texte und Sonderzeichen im Frankierstempeldruckbereich und ein beliebiges oder ein einer Kostenstelle zugeordnetes Werbeklischee zu drucken. So hat zum Beispiel die Frankiermaschine T1000 der Anmelderin einen Mikroprozessor, welcher von einem gesicherten Gehäuse umgeben ist, das eine Öffnung für die Zuführung eines Briefes aufweist. Bei einer Briefzuführung übermittelt ein mechanischer Briefsensor (Mikroschalter) ein

Druckanforderungssignal an den Mikroprozessor. Der Frankierabdruck beinhaltet eine zuvor eingegebene und gespeicherte postalische Information zur Beförderung des Briefes. Die Steuereinheit der Frankiermaschine nimmt eine Abrechnung softwaremäßig vor, übt eine Überwachungsfunktion ggf. bezüglich der Bedingungen für eine Datenaktualisierung aus und steuert das Nachladen eines Portwertguthabens.

Für die oben genannte Thermotransfer-Frankiermaschine wurde bereits in US 5,606,508 (DE 42 13 278 B1) und in US 5,490,077 eine Dateneingabemöglichkeit mittels Chipkarten vorgeschlagen. Eine der Chipkarten lädt neue Daten in die Frankiermaschine und ein Satz an weiteren Chipkarten gestattet durch das Stecken einer Chipkarte eine Einstellung entsprechend eingespeicherter Daten vorzunehmen. Das Datenladen und die Einstellung der Frankiermaschine kann damit bequemer und schneller als per Tastatureingabe erfolgen. Eine Frankiermaschine zum Frankieren von Postgut, ist mit einem Drucker zum Drucken des Postwertstempels auf das Postgut, mit einer Steuerung zum Steuern des Druckens und der peripheren Komponenten der Frankiermaschine, mit einer Abrecheneinheit zum Abrechnen von Postgebühren, mit mindestens einem nichtflüchtigen Speicher zum Speichern von Postgebührendaten, mit mindestens einem nichtflüchtigen Speicher zum Speichern von sicherheitsrelevanten Daten und mit einer Kalender/Uhr ausgestattet. Der nichtflüchtige Speicher der sicherheitsrelevanten Daten und/oder die Kalender/Uhr wird gewöhnlich von einer Batterie gespeist. Bei bekannten Frankiermaschinen werden sicherheitsrelevante Daten (kryptografische Schlüssel u.ä.) in nichtflüchtigen Speichern gesichert. Diese Speicher sind EEPROM, FRAM oder batteriegesicherte SRAM. Bekannte Frankiermaschinen verfügen oft auch über eine interne Echtzeituhr (Real Time Clock) RTC, die von einer Batterie gespeist wird. Bekannt sind z.B. vergossene Module, die integrierte Schaltkreise und eine Lithium-Batterie enthalten. Diese Module müssen nach Ablauf der Lebensdauer der Batterie im Ganzen ausgetauscht und entsorgt werden. Aus wirtschaftlichen und ökologischen Gesichtspunkten ist es günstiger, wenn nur die Batterie ausgetauscht werden muß. Dazu muß jedoch das Sicherheitsgehäuse geöffnet und anschließend wieder verschlossen und gesiegelt werden, denn die Sicherheit gegenüber Betrugsversuchen beruht im Wesentlichen auf dem gesicherten Gehäuse, welches die gesamte Maschine umschließt. Seitens der Anmelderin wurde in EP 660 269 A2 (US 5,671,146) bereits

ein geeignetes Verfahren zur Verbesserung der Sicherheit von Frankiermaschinen vorgeschlagen, in welchem zwischen einem autorisierten und unautorisierten Öffnen des Sicherheitsgehäuses unterschieden wird.

5

Eine eventuell erforderliche Reparatur einer Frankiermaschine ist dann vor Ort nur schwer möglich, wenn der Zugang zu den Bauteilen erschwert oder eingeschränkt ist. Bei größeren Postverarbeitungsmaschinen oder sogenannten PC-Frankierern wird zukünftig das gesicherte Gehäuse auf das sogenannte postalische Sicherheitsmodul reduziert werden, was die Zugänglichkeit zu den übrigen Bauteilen verbessern kann. Zum wirtschaftlichen Austauschen der Batterie des Sicherheitsmoduls wäre es außerdem wünschenswert, daß sich diese auf relativ einfachem Wege auswechseln läßt. Dazu muß sich die Batterie außerhalb des Sicherheitsbereichs der Frankiermaschine befinden. Wenn die Batterieklemmen aber von außen zugänglich gemacht werden, ist ein möglicher Angreifer in der Lage, die Batteriespannung zu manipulieren. Bekannte batteriegespeiste SRAM und RTC haben bzgl. ihrer geforderten Betriebsspannung unterschiedliche Anforderungen. Die notwendige Spannung zum Halten von Daten von SRAM liegt unterhalb der geforderten Spannung zum Betrieb von RTC. Daß bedeutet, daß ein Verringern der Spannung unter einen bestimmten Grenzwert zu einem unerwünschten Verhalten der Komponenten führt: Die RTC bleibt stehen, die Uhrzeit - gespeichert in SRAM-Zellen - und die Speicherinhalte des SRAM bleiben erhalten. Wenigstens eine der Sicherheitsmaßnahmen, beispielsweise Long Time Watchdogs, wären dann auf der Frankiermaschinenenseite unwirksam. Unter Long Time Watchdogs wird folgendes verstanden: Die entfernte Datenzentrale gibt einen Zeitkredit bzw. eine Zeitdauer, insbesondere eine Anzahl von Tagen, oder einen bestimmten Tag vor, bis zu welchem sich die Frankiereinrichtung per Kommunikationsverbindung melden kann. Nach erfolglosen Ablauf des Zeitkredits oder der Frist wird das Frankieren verhindert. Unter dem Titel: Verfahren und Anordnung zur Erzeugung und Überprüfung eines Sicherheitsabdruckes wurde bereits in der EP 660 270 A2 (US 5,680,463) ein Verfahren vorgeschlagen, die voraussichtliche Zeitdauer bis zur nächsten Guthabennachladung zu ermitteln, wobei seitens einer Datenzentrale diejenige Frankiermaschine als suspekt gilt, welche sich nicht fristgemäß meldet. Suspekte Frankiermaschinen werden der Postbehörde mitgeteilt, welche den Poststrom nach von suspekten Frankiermaschinen frankierten Briefen überwacht. Ein Ablauf des Zeitkredits

10  
15  
20  
25  
30  
35

oder der Frist wird bereits auch von der Frankiereinrichtung ermittelt und der Benutzer wird aufgefordert die überfällige Kommunikation durchzuführen.

- 5 Sicherheitsmodule sind von elektronischen Datenverarbeitungsanlagen her bereits bekannt. Zum Schutz vor Einbruch in eine elektronische Anlage wird in EP 417 447 B1 bereits eine Sperre vorgeschlagen, welche Stromversorgungsmittel- und Signalerfassungsmittel sowie Abschirmmittel im Gehäuse umfaßt. Das Abschirmmittel besteht aus Einkapselungs-  
10 material und Leitungsmitteln, an welchen die Stromversorgungs- und Signalerfassungsmittel angeschlossen sind. Letzteres reagiert auf eine Veränderung des Leitungswiderstandes des Leitungsmittels. Außerdem enthält das Sicherheitsmodul eine interne Batterie, einen Spannungs-  
15 umschalter von Systemspannung auf Batteriespannung, ein Power Gate und einen Kurzschlußtransistor sowie weitere Sensoren. Wenn die Spannung eine bestimmte Grenze unterschreitet, reagiert das Power Gate. Wenn der Leitungswiderstand, die Temperatur oder die Strahlung verändert ist, reagiert die Logik. Mittels des Power Gate oder mittels der  
20 Logik wird der Ausgang des Kurzschlußtransistor auf L-Pegel umgeschaltet, wodurch ein im Speicher gespeicherter kryptographischer Schlüssel gelöscht wird. Jedoch ist die Lebensdauer der nicht auswechselbaren Batterie und damit des Sicherheitsmoduls für den Einsatz in Frankiereinrichtungen bzw. Postverarbeitungsmaschinen zu klein.
- 25 Eine größere Postverarbeitungsmaschine ist beispielsweise die JetMail®. Ein Frankierdruck wird hier mittels einem stationär angeordneten Tintenstrahldruckkopf bei einem nichtwaagerechten annähernd vertikalen Brieftransport erzeugt. Eine geeignete Ausführung für eine Druckvorrichtung wurde bereits in der DE 196 05 015 C1 vorgeschlagen.  
30 Die Postverarbeitungsmaschine hat ein Meter und eine Base. Soll das Meter mit einem Gehäuse ausgestattet werden, so daß Bauteile leichter zugänglich sind, dann muß es durch ein postalisches Sicherheitsmodul vor Betrugsversuchen geschützt werden, welches mindestens das Abrechnen der Postgebühren durchführt. Um Einflüsse auf den Programm-  
35 verlauf auszuschließen, wurde bereits in der EP 789 333 A2 unter dem Titel: Frankiermaschine vorgeschlagen, ein Sicherheitsmodul mit einer Anwenderschaltung (Application Specific Integrated Circuit) ASIC auszustatten, die eine Hardware-Abrecheneinheit aufweist. Die Anwenderschaltung steuert außerdem die Druckdatenübertragung zum Druckkopf.

Letzteres wäre nur dann nicht erforderlich, wenn für jedes Poststück  
einzigartige Abdrucke erzeugt werden. Ein geeignetes Verfahren und  
Anordnung zur Erzeugung und Überprüfung eines Sicherheitsabdruckes  
ist beispielsweise in den US 5,680,463, US 5,712,916 und US 5,734,723  
5 vorgeschlagen worden. Dabei wird eine spezielle Sicherheitsmarkierung  
elektronisch generiert und in das Druckbild eingebettet.

Weitere Maßnahmen zum Schutz eines Sicherheitsmodul vor einem  
Angriff auf die in ihm gespeicherten Daten wurden auch in den nicht  
10 vorveröffentlichten deutschen Anmeldungen 198 16 572.2 und 198 16  
571.4 vorgeschlagen. Bei einer Vielzahl von Sensoren steigt der  
Stromverbrauch und ein nicht ständig von einer Systemspannung  
versorgter Sicherheitsmodul zieht dann den für die Sensoren benötigten  
Strom aus seiner internen Batterie, was letztere ebenfalls frühzeitig er-  
15 schöpft. Die Kapazität der Batterie und der Stromverbrauch beschränken  
somit die Lebensdauer eines Sicherheitsmoduls.

Frankiermaschinen sind wie viele andere Produkte ebenfalls modular  
aufgebaut. Diese Modularität ermöglicht den Austausch von Modulen und  
20 Komponenten aus verschiedenen Gründen. So können z.B. defekte  
Module ausgetauscht und durch überprüfte, reparierte oder neue Module  
ersetzt werden. Da eine höchste Sorgsamkeit beim Austausch von  
Baugruppen erforderlich ist, die sicherheitsrelevante Daten enthalten,  
erfordert der Austausch in der Regel den Einsatz eines Service  
25 Technikers und Maßnahmen, die bei unsachgemäßem Gebrauch bzw.  
unauthorisiertem Austausch eines Sicherheitsmoduls dessen Funktions-  
weise unterbinden. Letzteres ist aber sehr aufwendig.

Der Erfindung liegt die Aufgabe zugrunde, mit geringem Aufwand den  
30 Schutz vor einem unbefugt manipulierten Sicherheitsmodul zu gewähr-  
leisten, wenn das Sicherheitsmodul austauschbar angeordnet ist. Der  
Austausch soll von jederman auf möglichst einfache Weise möglich sein.

Die Aufgabe wird mit den Merkmalen des Verfahrens nach Anspruch 1  
35 und mit den Merkmalen der Anordnung nach Anspruch 3 gelöst.

Die Erfindung geht davon aus, mittels Funktionseinheiten den Austausch  
und Gebrauch eines Sicherheitsmoduls einer Frankiermaschine,

Postverarbeitungseinrichtung oder ähnlichen Gerätes festzustellen, um den Benutzern der verschiedenen Geräte eine Gewährleistung über die korrekte Funktionsweise des Sicherheitsmoduls und damit des gesamten Gerätes bieten zu können. Ein Austausch eines Sicherheitsmoduls wird  
5 mindestens detektiert und ggf. nachträglich als Zustand signalisiert, wenn der Sicherheitsmodul wieder gesteckt ist und mit einer Systemspannung versorgt wird. Die Veränderungen des Zustandes des Sicherheitsmoduls werden mittels einer ersten Funktionseinheit und mittels einer von einer Batterie versorgten Detektionseinheit erfaßt, welche eine rücksetzbare  
10 Selbsthaltung aufweist. Die erste Funktionseinheit kann den jeweiligen Zustand auswerten, wenn sie wieder mit Systemspannung versorgt wird. Die Vorteile liegen in einer schnellen Reaktion auf Veränderungen des Zustandes des Sicherheitsmoduls und in einem geringem Batteriestromverbrauch der Schaltung der Detektionseinheit während der  
15 Nichtversorgung des Sicherheitsmoduls mit der Systemspannung.

Es ist mindestens vom unsachgemäßem Gebrauch eines Sicherheitsmoduls bei jedem Austausch auszugehen, bei welchen nicht nur die Systemspannung fehlt, sondern auch die austauschbar angeordnete  
20 Batterie entfernt wird. Damit der Austausch von möglichst gering qualifiziertem Personal und in Zukunft gar durch den Benutzer ausgeführt werden kann, übernimmt eine weitere Funktionseinheit die Überwachung auf Spannungsausfall beim Austausch der Batterie, wobei die erste Funktionseinheit zunächst sensitive Daten löscht und damit den weiteren  
25 Gebrauch des Sicherheitsmoduls einschränkt oder gar unterbindet. Die erste Funktionseinheit erzwingt bei einer späteren Wiederinbetriebnahme eine Kontaktaufnahme des Sicherheitsmoduls mit einer entfernten Datenzentrale zum Freischalten mindestens einer Funktionseinheit. Falls  
30 der Sicherheitsmodul sachgemäß ausgetauscht wurde, werden bei der Wiederinbetriebnahme die sensitiven Daten reinitialisiert. Zur Kontaktaufnahme sind Verfahren mit einer digitalen oder analogen Übertragungsstrecke einsetzbar. Das Verfahren zum Schutz eines Sicherheitsmoduls beinhaltet die folgenden Schritte:

- Überwachung des sachgemäßen Gebrauchs oder Austausches des  
35 Sicherheitsmoduls mittels einer ersten, zweiten und dritten Funktionseinheit,
- Löschen von sensitiven Daten aufgrund eines unsachgemäßen Gebrauchs oder Austausches mindestens mittels der zweiten Funktionseinheit,

- Sperren der Funktionalität mittels der dritten Funktionseinheit während eines Austausches des Sicherheitsmoduls,
- Reinitialisieren mittels der ersten Funktionseinheit von zuvor gelöschten sensitiven Daten nach sachgemäßem Gebrauch oder Austausch des Sicherheitsmoduls,
- Wiederinbetriebnahme durch Freischalten der Funktionseinheiten des Sicherheitsmoduls.

Es ist vorgesehen, daß das Reinitialisieren in Verbindung mit einer Kommunikation mittels einer entfernten Datenzentrale von der ersten Funktionseinheit vorgenommen wird, nachdem eine dynamische Gestecktseindetektion erfolgreich durchgeführt wurde, wobei während der Detektion von der ersten Funktionseinheit über eine Stromschleife der Interfaceeinheit Informationen ausgetauscht werden, deren fehlerfreie Übermittlung den Beweis für den sachgemäßen Einbau des Sicherheitsmoduls erbringt. Das Freischalten von Funktionseinheiten des Sicherheitsmoduls erfolgt durch deren Rücksetzen. Die erste Funktionseinheit ist ein mit den anderen Funktionseinheiten verbundener Prozessor, welcher programmiert ist, den jeweiligen Zustand festzustellen. Die zweite Funktionseinheit ist eine Spannungsüberwachungseinheit mit rücksetzbarer Selbsthaltung und die dritte Funktionseinheit ist eine Ungestecktseindetektionsschaltung mit rücksetzbarer Selbsthaltung.

Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet bzw. werden nachstehend zusammen mit der Beschreibung der bevorzugten Ausführung der Erfindung anhand der Figuren näher dargestellt. Es zeigen:

Figur 1, Blockbild und Interface des Sicherheitsmoduls,

30

Figur 2, Blockschaltbild der Frankiermaschine,

Figur 3, Perspektivische Ansicht der Frankiermaschine von hinten,

Figur 4, Blockschaltbild des Sicherheitsmoduls (zweite Variante),

35

Figur 5, Schaltbild der Detektionseinheit,



Figur 6, Seitenansicht des Sicherheitsmoduls,

Figur 7, Draufsicht auf das Sicherheitsmodul,

5     Figur 8a, Ansicht des Sicherheitsmoduls von rechts,

Figur 8b, Ansicht des Sicherheitsmoduls von links.

10     In der Figur 1 ist ein Blockbild des Sicherheitsmoduls 100 mit den Kontaktgruppen 101, 102 zum Anschluß an ein Interface 8 sowie mit den Batteriekontaktklemmen 103 und 104 eines Batterieinterfaces für eine Batterie 134 dargestellt. Obwohl das Sicherheitsmodul 100 mit einer harten Vergußmasse vergossen ist, ist die Batterie 134 des Sicherheitsmoduls 100 außerhalb der Vergußmasse auf einer Leiterplatte auswechselbar angeordnet. Die Leiterplatte trägt die Batteriekontaktklemmen 103 und 104 für den Anschluß der Pole der Batterie 134. Mittels der Kontaktgruppen 101, 102 wird das Sicherheitsmodul 100 an ein entsprechendes Interface 8 der Hauptplatine (Motherboard) 9 gesteckt. Die erste Kontaktgruppe 101 steht mit dem Systembus einer Steuerungseinrichtung in Kommunikationsverbindung und die zweite Kontaktgruppe 102 dient der Versorgung des Sicherheitsmoduls 100 mit der Systemspannung. Über die Pins P3, P5-P19 der Kontaktgruppe 101 laufen Adreß- und Datenleitungen 117, 118 sowie Steuerleitungen 115. Die erste und/oder zweite Kontaktgruppe 101 und/oder 102 sind/ist zur statischen und dynamischen Überwachung des Angestecktseins des Sicherheitsmoduls 100 ausgebildet. Über die Pins P23 und P25 der Kontaktgruppe 102 wird die Versorgung des Sicherheitsmodul 100 mit der Systemspannung der Hauptplatine 9 realisiert und über die Pins P1, P2 bzw. P4 wird eine dynamische und statische Ungestecktsein-Detektion durch das Sicherheitsmodul 100 realisiert.

30     Das Sicherheitsmodul 100 weist in an sich bekannter Weise einen Mikroprozessor 120 auf, der einen - nicht gezeigten - integrierten Festwertspeicher (internal ROM) mit dem speziellen Anwendungsprogramm enthält, was für die Frankiermaschine von der Postbehörde bzw. vom jeweiligen Postbeförderer zugelassen ist. Alternativ kann an den internen Datenbus 126 ein üblicher Festwertspeicher ROM oder FLASH-Speicher angeschlossen werden.

Das Sicherheitsmodul 100 weist in an sich bekannter Weise eine Reset-Schaltungseinheit 130, einen Anwenderschaltkreis ASIC 150 und eine Logik PAL 160 auf, die für den ASIC als Steuersignalgenerator dient. Die Reset-Schaltungseinheit 130 bzw. der Anwenderschaltkreis ASIC 150 und die Logik PAL 160 sowie eventuell weitere – nicht gezeigte – Speicher werden über die Leitungen 191 bzw. 129 mit Systemspannung  $U_{s+}$  versorgt, welche bei eingeschalteter Frankiereinrichtung von der Hauptplatine 9 geliefert wird. In der EP 789 333 A2 wurden bereits die wesentlichen Teile eines postalischen Sicherheitsmoduls PSM erläutert, die die Funktionen Abrechnen und Absichern der Postgebührendaten realisieren.

Die Systemspannung  $U_{s+}$  liegt außerdem über eine Diode 181 und die Leitung 136 am Eingang der Spannungsüberwachungseinheit 12 an. Am Ausgang der Spannungsüberwachungseinheit 12 wird eine zweite Betriebsspannung  $U_{b+}$  geliefert, welche über die Leitung 138 zur Verfügung steht. Bei ausgeschalteter Frankiereinrichtung steht nicht die Systemspannung  $U_{s+}$ , sondern nur die Batteriespannung  $U_{b+}$  zur Verfügung. Die am negativen Pol liegende Batteriekontaktklemme 104 ist mit Masse verbunden. Von der am positiven Pol liegenden Batteriekontaktklemme 103 wird Batteriespannung über eine Leitung 193, über eine zweite Diode 182 und die Leitung 136 an den Eingang der Spannungsüberwachungseinheit geliefert. Alternativ zu den beiden Dioden 181, 182 kann ein handelsüblicher Schaltkreis als Spannungsumschalter 180 eingesetzt werden.

Der Ausgang der Spannungsüberwachungseinheit 12 ist über eine Leitung 138 mit einem Eingang für diese zweite Betriebsspannung  $U_{b+}$  des Prozessors 120 verbunden, welcher mindestens auf einen RAM-Speicherbereich 122, 124 führt und dort eine nichtflüchtige Speicherung solange garantiert, wie die zweite Betriebsspannung  $U_{b+}$  in der erforderlichen Höhe anliegt. Der Prozessor 120 enthält vorzugsweise einen internen RAM 124 und eine Echtzeituhr (RTC) 122.

Die Spannungsüberwachungseinheit 12 im Sicherheitsmodul weist eine rücksetzbare Selbsthaltung auf, die vom Prozessor 120 über eine Leitung 164 abgefragt und über eine Leitung 135 zurückgesetzt werden kann. Für eine Rücksetzung der Selbsthaltung weist die Spannungsüberwachungseinheit 12 Schaltungsmittel auf. Die Rücksetzung ist erst auslösbar, wenn die Batteriespannung über die vorbestimmte Schwelle angestiegen ist.

Die Leitungen 135 und 164 sind je mit einem Pin (Pin1 und 2) des Prozessors 120 verbunden. Die Leitung 164 liefert ein Statussignal an den Prozessor 120 und die Leitung 135 liefert ein Steuersignal an die Spannungsüberwachungseinheit 12.

5

Die Leitung 136 am Eingang der Spannungsüberwachungseinheit 12 versorgt zugleich eine Ungestecktsein-Detektionseinheit 13 mit Betriebs- oder Batteriespannung. Die Ungestecktsein-Detektionseinheit 13 gibt auf der Leitung 139 ein Statussignal an einen Pin 5 des Prozessors 120 ab,  
10 das eine Aussage über den Zustand der Schaltung gibt. Vom Prozessor 120 wird der Zustand der Ungestecktsein-Detektionseinheit 13 über die Leitung 139 abgefragt. Der Prozessor kann mit einem vom Pin 4 des Prozessors 120 über die Leitung 137 abgegebenen Signal die Ungestecktsein-Detektionseinheit 13 zurücksetzen. Nach dem Setzen wird eine  
15 statische Prüfung auf Anschluß durchgeführt. Dazu wird über eine Leitung 192 Massepotential abgefragt, welches am Anschluß P4 des Interfaces 8 des postalischen Sicherheitsmoduls PSM 100 anliegt und nur abfragbar ist, wenn der Sicherheitsmodul 100 ordnungsgemäß gesteckt ist. Bei gesteckten Sicherheitsmodul 100 wird Massepotential des negativen Pols  
20 104 der Batterie 134 des postalischen Sicherheitsmoduls PSM 100 auf den Anschluß P23 des Interfaces 8 gelegt und ist somit am Anschluß P4 des Interfaces 8 über die Leitung 192 von der Ungestecktsein-Detektionseinheit 13 abfragbar.

25 An den Pins 6 und 7 des Prozessors 120 liegt eine Leitungsschleife, welche über die Pins P1 und P2 der Kontaktgruppe 102 des Interfaces 8 zum Prozessor 120 zurückgeschleift wird. Zur dynamischen Prüfung des Angeschlossenseins des postalischen Sicherheitsmoduls PSM 100 an der Hauptplatine 9 werden vom Prozessor 120 wechselnde Signalpegel in  
30 ganz unregelmäßigen Zeitabständen an die Pins 6, 7 angelegt und über die Schleife zurückgeschleift.

Das postalische Sicherheitsmodul PSM 100 ist mit einer Long-Live-Batterie bestückt, welches auch eine Überwachung des Gebrauchs  
35 ermöglicht, ohne das das Sicherheitsmodul an einer Systemspannung eines Postverarbeitungseinrichtung liegt. Der sachgemäße Gebrauch, Betrieb, Installation oder Einbau in der geeigneten Umgebung sind solche

von den Funktionseinheiten des Sicherheitsmoduls zu prüfende Eigenschaften. Eine Erstinstallation wird vom Hersteller des postalischen Sicherheitsmoduls vorgenommen. Es ist also nach dieser Erstinstallation zunächst lediglich zu prüfen, ob das postalische Sicherheitsmodul von  
5 ihrem Einsatzfeld (Postverarbeitungseinrichtung) getrennt wird, wobei dies in der Regel bei einem Austausch erfolgt.

Die Überwachung dieses Zustandes wird von der Ungestecktsein-Detektionseinheit 13 vorgenommen. Hierbei wird über die Masseverbindung am Pin 4 der Interfaceeinheit 8 ein Spannungspegel überwacht.  
10 Beim Austausch der Funktionseinheit wird diese Masseverbindung unterbrochen und die Ungestecktsein-Detektionseinheit 13 registriert diesen Vorgang als Information. Da für jede Trennung des Sicherheitsmoduls 100 von der Interfaceeinheit 8, die Speicherung dieser Information durch den speziellen batteriegetriebenen Schaltungsaufbau gewährleistet ist,  
15 kann eine Auswertung dieser Information zu jeder Zeit erfolgen, falls eine Wiederinbetriebnahme gewünscht ist. Die regelmäßige Auswertung dieses Ungestecktsein-Signals auf der Leitung 139 der Ungestecktsein-Detektionseinheit 13 ermöglicht es dem Prozessor 120 sensitive Daten zu löschen, ohne jedoch damit die Abrechnungs- und Kundendaten in den  
20 NVRAM-Speichern zu verändern. Der momentane Zustand des postalischen Sicherheitsmoduls mit den gelöschten sensitiven Daten kann als Wartungszustand aufgefaßt werden, in welchem in der Regel der Austausch, eine Reparatur oder sonstiges vorgenommen wird. Da die sensitiven Daten der Funktionseinheit gelöscht sind, ist ein Fehler aufgrund  
25 einer unsachgemäßen Handhabung des postalischen Sicherheitsmoduls ausgeschlossen. Die sensitiven Daten sind beispielsweise kryptographische Schlüssel. Der Prozessor 120 verhindert im Wartungszustand eine Kernfunktionalität des postalischen Sicherheitsmoduls, welche beispielsweise in der Abrechnung und/oder Berechnung eines Sicherheitscodes  
30 für die Sicherheitsmarkierung in einem Sicherheitsabdruck besteht.

Zur Wiederinbetriebnahme wird das postalische Sicherheitsmodul PSM zunächst gesteckt und elektrisch mit der entsprechenden Interfaceeinheit 8 eines Postbearbeitungsgerätes verbunden. Anschließend wird das Gerät eingeschaltet und somit das postalische Sicherheitsmodul wieder  
35 mit Systemspannung  $U_{s+}$  versorgt. Aufgrund des speziellen Zustandes muß nun der sachgemäße Einbau des postalischen Sicherheitsmoduls durch ihre Funktionseinheit erneut geprüft werden. Hierfür wird eine

zweite Stufe einer Prüfung (dynamische Gestecktsein-Detektion) vorgesehen. Über eine zwischen der ersten Funktionseinheit (Prozessor 120) und der Stromschleife 18 der Interfaceeinheit 8 hergestellten operative Verbindung werden Informationen ausgetauscht, deren fehlerfreie Übermittlung den Beweis für den sachgemäßen Einbau erbringt. Dies ist Voraussetzung für eine erfolgreiche Wiederinbetriebnahme.

Für den Zustandswechsel in den normalen Betriebszustand ist nun noch eine Reinitialisierung der sensitiven Daten erforderlich. Zwischen dem postalischen Sicherheitsmodul und einer dritten Instanz wird eine Kommunikation vorgenommen, wobei letztere diese sensitiven Daten übermittelt. Nach erfolgreicher Übermittlung wird die Ungestecktsein-Detektionseinheit 13 zurückgesetzt und das postalische Sicherheitsmodul nimmt wieder seinen normalen Betriebszustand ein. Die Wiederinbetriebnahme ist abgeschlossen.

Die Figur 2 zeigt ein Blockschaltbild einer Frankiermaschine, die mit einer Chipkarten-Schreib/Leseeinheit 70 zum Nachladen von Änderungsdaten per Chipkarte und mit einer Druckeinrichtung 2, welche von einer Steuereinrichtung 1 gesteuert wird, ausgestattet ist. Die Steuereinrichtung 1 weist ein mit einem Mikroprozessor 91 mit zugehörigen Speichern 92, 93, 94, 95 ausgestattetes Motherboard 9 auf.

Der Programmspeicher 92 enthält ein Betriebsprogramm mindestens zum Drucken und wenigstens sicherheitsrelevante Bestandteile des Programms für eine vorbestimmte Format-Änderung eines Teils der Nutzdaten.

Der Arbeitsspeicher RAM 93 dient zur flüchtigen Zwischenspeicherung von Zwischenergebnissen. Der nichtflüchtige Speicher NVM 94 dient zur nichtflüchtigen Zwischenspeicherung von Daten, beispielsweise von statistischen Daten, die nach Kostenstellen geordnet sind. Der Kalender/Uhrenbaustein 95 enthält ebenfalls adressierbare aber nichtflüchtige Speicherbereiche zur nichtflüchtigen Zwischenspeicherung von Zwischenergebnissen oder auch bekannten Programmteilen (beispielsweise für den DES-Algorithmus). Es ist vorgesehen, daß die Steuereinrichtung 1 mit der Chipkarten-Schreib/Leseeinheit 70 verbunden ist, wobei der Mikroprozessor 91 der Steuereinrichtung 1 beispielsweise dazu programmiert ist, die Nutzdaten N aus dem Speicherbereich einer Chipkarte 49 zu deren Anwendung in entsprechende Speicherbereiche

der Frankiermaschine zu laden. Eine in einen Einsteckschlitz 72 der Chipkarten-Schreib/Leseeinheit 70 eingesteckte erste Chipkarte 49 gestattet ein Nachladen eines Datensatzes in die Frankiermaschine für mindestens eine Anwendung. Die Chipkarte 49 enthält beispielsweise die

5 Portogebühren für alle üblichen Postbefördererleistungen entsprechend des Tarifs der Postbehörde und ein Postbefördererkennzeichen, um mit der Frankiermaschine ein Stempelbild zugenerieren und entsprechend des Tarifs der Postbehörde die Poststücke freizustempeln.

10 Die Steuereinrichtung 1 bildet das eigentliche Meter mit den Mitteln 91 bis 95 der vorgenannten Hauptplatine 9 und umfaßt auch eine Tastatur 88, eine Anzeigeeinheit 89 sowie einen anwendungsspezifischen Schaltkreis ASIC 90 und das Interface 8 für das postalische Sicherheitsmodul PSM 100. Das Sicherheitsmodul PSM 100 ist über einen Steuerbus mit dem

15 vorgenannten ASIC 90 und dem Mikroprozessor 91 sowie über den parallelen µC-Bus mindestens mit den Mitteln 91 bis 95 der Hauptplatine 9 und der mit Anzeigeeinheit 89 verbunden. Der Steuerbus führt Leitungen für die Signale CE, RD und WR zwischen dem Sicherheitsmodul PSM 100 und dem vorgenannten ASIC 90. Der Mikroprozessor 91

20 weist vorzugsweise einen Pin für ein vom Sicherheitsmodul PSM 100 abgegebenes Interruptsignal i, weitere Anschlüsse für die Tastatur 88, eine serielle Schnittstelle SI-1 für den Anschluß der Chipkarten-Schreib/Lese-Einheit 70 und eine serielle Schnittstelle SI-2 für den optionalen Anschluß eines MODEMs auf. Mittels des MODEMs kann

25 beispielsweise das im nichtflüchtigen Speicher des postalischen Sicherheitsmittels PSM 100 gespeicherte Guthaben erhöht werden.

Das postalische Sicherheitsmittel PSM 100 wird von einem gesicherten Gehäuse umschlossen. Vor jedem Frankierabdruck wird im postalischen

30 Sicherheitsmodul PSM 100 eine hardwaremäßige Abrechnung durchgeführt. Die Abrechnung erfolgt unabhängig von Kostenstellen. Das postalische Sicherheitsmittel PSM 100 kann intern so ausgeführt sein, wie in der europäischen Anmeldung EP 789 333 A3 näher beschrieben wurde.

35 Es ist vorgesehen, daß der ASIC 90 eine serielle Schnittstellenschaltung 98 zu einem im Poststrom vorschalteten Gerät, eine serielle Schnittstellenschaltung 96 zu den Sensoren und Aktoren der Druckeinrichtung 2, eine serielle Schnittstellenschaltung 97 zur Drucksteuerelektronik 16 für den Druckkopf 4 und eine serielle

Schnittstellenschaltung 99 zu einem der Druckeinrichtung 20 im Poststrom nachgeschalteten Gerät aufweist. Der DE 197 11 997 ist eine Ausführungsvariante für die Peripherieschnittstelle entnehmbar, welche für mehrere Peripheriegeräte (Stationen) geeignet ist. Sie trägt den Titel:  
5 Anordnung zur Kommunikation zwischen einer Basisstation und weiteren Stationen einer Postbearbeitungsmaschine und zu deren Notabschaltung.

Die Schnittstellenschaltung 96 gekoppelt mit der in der Maschinenbasis befindlichen Schnittstellenschaltung 14 stellt mindestens eine Verbindung  
10 zu den Sensoren 6, 7, 17 und zu den Aktoren, beispielsweise zum Antriebsmotor 15 für die Walze 11 und zu einer Reinigungs- und Dichtstation RDS 40 für den Tintenstrahldruckkopf 4, sowie zum Labelgeber 50 in der Maschinenbasis her. Die prinzipielle Anordnung und das Zusammenspiel zwischen Tintenstrahldruckkopf 4 und der RDS 40  
15 sind der DE 197 26 642 C2 entnehmbar, mit dem Titel: Anordnung zur Positionierung eines Tintenstrahldruckkopfes und einer Reinigungs- und Dichtvorrichtung.

Einer der in der Führungsplatte 20 angeordneten Sensoren 7, 17 ist der Sensor 17 und dient zur Vorbereitung der Druckauslösung beim Brieftransport. Der Sensor 7 dient zur Briefanfangserkennung zwecks Druckauslösung beim Brieftransport. Die Transporteinrichtung besteht aus einem Transportband 10 und zwei Walzen 11, 11'. Eine der Walzen ist die mit einem Motor 15 ausgestattete Antriebswalze 11, eine andere ist die mitlaufende Spannwalze 11'. Vorzugsweise ist die Antriebswalze 11 als  
25 Zahnwalze ausgeführt, entsprechend ist auch das Transportband 10 als Zahnriemen ausgeführt, was die eindeutige Kraftübertragung sichert. Ein Encoder 5, 6 ist mit einer der Walzen 11, 11' gekoppelt. Vorzugsweise sitzt die Antriebswalze 11 mit einem Inkrementalgeber 5 fest auf einer Achse. Der Inkrementalgeber 5 ist beispielsweise als Schlitzscheibe ausgeführt, die mit einer Lichtschranke 6 zusammen wirkt, und gibt über  
30 die Leitung 19 ein Encodersignal an die Hauptplatine 9 ab.

Es ist vorgesehen, daß die einzelnen Druckelemente des Druckkopfes innerhalb seines Gehäuses mit einer Druckkopfelektronik verbunden sind und daß der Druckkopf für einen rein elektronischen Druck ansteuerbar  
35 ist. Die Drucksteuerung erfolgt auf Basis der Wegsteuerung, wobei der gewählte Stempelversatz berücksichtigt wird, welcher per Tastatur 88 oder bei Bedarf per Chipkarte eingegeben und im Speicher NVM 94 nichtflüchtig gespeichert wird. Ein geplanter Abdruck ergibt sich somit aus Stempelversatz (ohne Drucken), dem Frankierdruckbild und gegebenenfalls

weiteren Druckbildern für Werbeklischee, Versandinformationen (Wahl-  
drucke) und zusätzlichen editierbaren Mitteilungen. Der nichtflüchtige  
Speicher NVM 94 weist eine Vielzahl an Speicherbereichen auf. Darunter  
sind solche, welche die geladenen Portogebührentabellen nichtflüchtig  
5 speichern.

Die Chipkarten-Schreib/Leseeinheit 70 besteht aus einem zugehörigen  
mechanischen Träger für die Mikroprozessorkarte und Kon-taktiereinheit  
74. Letztere gestattet eine sichere mechanische Halterung der Chipkarte  
in Lese-Position und eindeutige Signalisierung des Erreichens der  
10 Lese-Position der Chipkarte in der Kontaktierungseinheit. Die  
Mikroprozessorkarte mit dem Mikroprozessor 75 besitzt eine einpro-  
grammierte Lesefähigkeit für alle Arten von Speicherkarten bzw. Chip-  
karten. Das Interface zur FM ist eine serielle Schnittstelle gemäß RS232-  
Standard. Die Datenübertragungsrate beträgt min. 1,2 K Baud. Das  
15 Einschalten der Stromversorgung erfolgt mittels einem an der Haupt-  
platine angeschlossenen Schalter 71. Nach Einschalten der Stromver-  
sorgung erfolgt eine Selbsttestfunktion mit Bereitschaftsmeldung.

In der Figur 3 ist eine perspektivische Ansicht der Frankiermaschine von  
20 hinten dargestellt. Die Frankiermaschine besteht aus einem Meter 1 und  
einer Base 2. Letztere ist mit einer Chipkarten-Schreib/ Leseeinheit 70  
ausgestattet, die hinter der Führungsplatte 20 angeordnet und von der  
Gehäuseoberkante 22 zugänglich ist. Nach dem Einschalten der Frankier-  
maschine mittels dem Schalter 71 wird eine Chipkarte 49 von oben nach  
25 unten in den Einsteckschlitz 72 eingesteckt. Ein zugeführter auf der Kante  
stehender Brief 3, der mit seiner zu bedruckenden Oberfläche an der  
Führungsplatte anliegt, wird dann entsprechend der Eingabedaten mit  
einem Frankierstempel 31 bedruckt. Die Briefzuführöffnung wird durch  
eine Klarsichtplatte 21 und die Führungsplatte 20 seitlich begrenzt. Die  
30 Statusanzeige des auf die Hauptplatine 9 des Meters 1 gesteckten  
Sicherheitsmoduls 100 ist von außen durch eine Öffnung 109 sichtbar.

Die Figur 4 zeigt ein Blockschaltbild des postalischen Sicherheitsmoduls  
PSM 100 in einer bevorzugten Variante. Der negative Pol der Batterie 134  
35 ist auf Masse und einen Pin P23 der Kontaktgruppe 102 gelegt. Der  
positive Pol der Batterie 134 ist über die Leitung 193 mit dem einen  
Eingang des Spannungsumschalters 180 und die Systemspannung  
führende Leitung 191 ist mit dem anderen Eingang des Spannungs-  
umschalters 180 verbunden. Als Batterie 134 eignet sich der Typ SL-



- 389/P für eine Lebensdauer bis zu 3,5 Jahren oder der Typ SL-386/P für eine Lebensdauer bis zu 6 Jahren bei einem maximalen Stromverbrauch durch das PSM 100. Als Spannungsumschalter 180 kann ein handelsüblicher Schaltkreis vom Typ ADM 8693ARN eingesetzt werden.
- 5 Der Ausgang des Spannungsumschalters 180 liegt über die Leitung 136 an der Batterieüberwachungseinheit 12 und der Detektionseinheit 13 an. Die Batterieüberwachungseinheit 12 und die Detektionseinheit 13 stehen mit den Pins 1, 2, 4 und 5 des Prozessors 120 über die Leitungen 135, 164 und 137, 139 in Kommunikationsverbindung. Der Ausgang des
- 10 Spannungsumschalters 180 liegt über die Leitung 136 außerdem am Versorgungseingang eines ersten Speichers SRAM an, der durch die vorhandene Batterie 134 zum nichtflüchtigen Speicher NVRAM einer ersten Technologie wird.
- Das Sicherheitsmodul steht mit der Frankiermaschine über den
- 15 Systembus 115, 117, 118 in Verbindung. Der Prozessor 120 kann über den Systembus und ein Modem 83 in Kommunikationsverbindung mit einer entfernten Datenzentrale eintreten. Die Abrechnung wird vom ASIC 150 vollzogen und vom Prozessor 120 überprüft. Die postalischen Abrechnungsdaten werden in nichtflüchtigen Speichern unterschiedlicher
- 20 Technologie gespeichert.
- Die Systemspannung liegt am Versorgungseingang eines zweiten Speichers NV-RAM 114 an. Bei letzterem handelt es sich um einen nichtflüchtigen Speicher NVRAM einer zweiten Technologie, (SHADOW-RAM). Diese zweiten Technologie umfaßt vorzugsweise ein RAM und ein
- 25 EEPROM, wobei letzteres die Dateninhalte bei Systemspannungsausfall automatisch übernimmt. Der NVRAM 114 der zweiten Technologie ist mit den entsprechenden Adress- und Dateneingängen des ASIC's 150 über einen internen Adreß- und Datenbus 112, 113 verbunden.
- 30 Der ASIC 150 enthält mindestens eine Hardware-Abrecheneinheit für die Berechnung der zu speichernden postalischen Daten. In der Programmable Array Logic (PAL) 160 ist eine Zugriffslogik auf den ASIC 150 untergebracht. Der ASIC 150 wird durch die Logik PAL 160 gesteuert. Ein Adreß- und Steuerbus 117, 115 von der Hauptplatine 9 ist an
- 35 entsprechenden Pins der Logik PAL 160 angeschlossen und die PAL 160 erzeugt mindestens ein Steuersignal für das ASIC 150 und ein Steuersignal 119 für den Programmspeicher FLASH 128. Der Prozessor 120 arbeitet ein Programm ab, das im FLASH 128 gespeichert ist. Der Prozessor 120, FLASH 28, ASIC 150 und PAL 160 sind über einen

modulinternen Systembus miteinander verbunden, der Leitungen 110,111,126,119 für Daten-, Adreß- und Steuersignale enthält.

Der Prozessor 120 des Sicherheitsmoduls 100 ist über einen modulinternen Datenbus 126 mit einem FLASH 128 und mit dem ASIC 150 verbunden. Der FLASH 128 wird mit Systemspannung Us+ versorgt. Er ist beispielsweise ein 128 Kbyte- FLASH-Speicher vom Typ AM29F010-45EC. Der ASIC 150 des postalischen Sicherheitsmoduls 100 liefert über einen modulinternen Adreßbus 110 die Adressen 0 bis 7 an die entsprechenden Adreßeingänge des FLASH 128. Der Prozessor 120 des Sicherheitsmoduls 100 liefert über einen internen Adreßbus 111 die Adressen 8 bis 15 an die entsprechenden Adresseingänge des FLASH 128. Der ASIC 150 des Sicherheitsmoduls 100 steht über die Kontaktgruppe 101 des Interfaces 8 mit dem Datenbus 118, mit dem Adreßbus 117 und dem Steuerbus 115 des Motherbords 9 in Kommunikationsverbindung.

Es ist vorgesehen, daß der Prozessor 120 Speicher 122, 124 aufweist, an welche über die Leitung 138 eine Betriebsspannung Ub+ von einer Spannungsüberwachungseinheit 12 zugeführt wird. Insbesondere eine Echtzeituhr RTC 122 und der Speicher RAM 124 werden von einer Betriebsspannung über die Leitung 138 versorgt. Die Spannungsüberwachungseinheit (Battery Observer) 12 liefert außerdem ein Statussignal 164 und reagiert auf ein Steuersignal 135. Der Spannungsumschalter 180 gibt als Ausgangsspannung auf der Leitung 136 für den Battery Observer 12 und Speicher 116 diejenige seiner Eingangsspannungen als Versorgungsspannung weiter, die größer als die andere ist. Durch die Möglichkeit, die beschriebene Schaltung in Abhängigkeit von der Höhe der Spannungen Us+ und Ub+ automatisch mit der größeren von beiden zu speisen, kann während des Normalbetriebs die Batterie 134 ohne Datenverlust gewechselt werden.

Die Batterie 134 des Sicherheitsmoduls 100 speist in den Ruhezeiten außerhalb des Normalbetriebes in vorerwähnter Weise die Echtzeituhr (RTC) 122 mit Datums und/oder Uhrzeitregistern und/oder den statischen RAM (SRAM) 124, der sicherheitsrelevante Daten hält. Sinkt die Spannung der Batterie während des Batteriebetriebs unter eine bestimmte Grenze, so wird von der Spannungsüberwachungseinheit 12 der Speisepunkt für die RTC und SRAM bis zum Rücksetzen mit Masse verbunden. Die Spannung an der RTC und am SRAM liegt dann bei 0V. Das führt

dazu, daß der SRAM 124, der z.B. wichtige kryptografische Schlüssel enthält, sehr schnell gelöscht wird. Gleichzeitig werden auch die Register der RTC 122 gelöscht und die aktuelle Uhrzeit und das aktuelle Datum gehen verloren. Durch diese Aktion wird verhindert, daß ein möglicher  
5 Angreifer durch Manipulation der Batteriespannung die frankiermaschineninterne Uhr 122 anhält, ohne daß sicherheitsrelevante Daten verloren gehen. Somit wird verhindert, daß der Angreifer Sicherheitsmaßnahmen, wie beispielsweise Long Time Watchdogs umgeht.

10 Die RESET-Einheit 130 ist über die Leitung 131 mit dem Pin 3 des Prozessors 120 und mit einem Pin des ASIC's 150 verbunden. Der Prozessor 120 und das ASIC 150 werden bei Absinken der Versorgungsspannung durch eine Resetgenerierung in der RESET-Einheit 130 zurückgesetzt.

15 Gleichzeitig mit der Indikation der Unterspannung der Batterie wechselt die beschriebene Schaltung in einen Selbsthaltezustand, in dem sie auch bei nachträglicher Erhöhung der Spannung bleibt. Beim nächsten Einschalten des Moduls kann der Prozessor den Zustand der Schaltung  
20 abfragen (Statussignal) und damit und/oder über die Auswertung der Inhalte des gelöschten Speichers darauf schließen, daß die Batteriespannung zwischenzeitlich einen bestimmten Wert unterschritten hat. Der Prozessor kann die Überwachungsschaltung zurücksetzen, d.h. "scharf" machen.

25 Die Ungestecktsein-Detektionseinheit 13 hat zur Messung der Eingangsspannung eine Leitung 192, die über den Stecker des Sicherheitsmoduls und Interface 8, vorzugsweise über einen Sockel auf der Mutterplatine 9 der Frankiermaschine mit Masse verbunden ist. Diese Messung dient zur  
30 statischen Überwachung des Gesteckseins und bildet die Grundlage für eine Überwachung auf einer ersten Stufe. Es ist vorgesehen, daß die Ungestecktsein-Detektionseinheit 13 Schaltungsmittel für eine rücksetzbare Selbsthaltung aufweist, wobei die Selbsthaltung ausgelöst wird, wenn der Spannungspegel auf einer Meßspannungsleitung 192 von  
35 einem vorbestimmten Potential abweicht. Zugleich umfaßt die Auswertelogik den mit den anderen Funktionseinheiten verbundenen Prozessor 120, welcher programmiert ist, den jeweiligen Zustand des Sicherheitsmoduls 100 festzustellen und zu verändern. Der Zustand der

Selbsthaltung ist über die Leitung 139 vom Prozessor 120 des Sicherheitsmoduls 100 abfragbar. Das Meßspannungspotential auf der Leitung 192 entspricht Massepotential, wenn der Sicherheitsmodul 100 ordnungsgemäß gesteckt ist. Auf der Leitung 139 liegt Betriebsspannungspotential. Massespannungspotential liegt auf der Leitung 139 an, wenn der Sicherheitsmodul 100 ungesteckt ist. Der Prozessor 120 weist einen fünften Pin5 auf, an welchem die Leitung 139 angeschlossen ist, um den Zustand der Ungestecktsein-Detektionseinheit 13 abzufragen, ob sie auf Massepotential mit Selbsthaltung geschaltet ist. Um den Zustand der Selbsthaltung der Ungestecktsein-Detektionseinheit 13 über die Leitung 137 zurückzusetzen, weist der Prozessor 120 einen vierten Pin 4 auf.

Weiterhin ist eine Stromschleife 18 vorgesehen, die die Pins 6 und 7 des Prozessors 120 ebenfalls über den Stecker des Sicherheitsmoduls und über den Sockel auf der Hauptplatine 9 der Frankiermaschine miteinander verbindet. Die Leitungen an den Pins 6 und 7 des Prozessors 120 sind nur bei einem an die Hauptplatine 9 gesteckten PSM 100 zu einer Stromschleife 18 geschlossen. Diese Schleife bildet die Grundlage für eine dynamische Überwachung des Angestecktseins des Sicherheitsmoduls auf einer zweiten Stufe.

Der Prozessor 120 weist intern eine Verarbeitungseinheit CPU 121, eine Echtzeituhr RTC 122 eine RAM-Einheit 124 und eine Ein/Ausgabe-Einheit 125 auf. Der Prozessor 120 ist mit Pin's 8, 9 zur Ausgabe mindestens eines Signals zur Signalisierung des Zustandes des Sicherheitsmoduls 100 ausgestattet. An den Pins 8 und 9 liegen I/O-Ports der Ein/Ausgabe-Einheit 125, an welchen modulinterne Signalmittel angeschlossen sind, beispielsweise farbige Lichtemitterdioden LED's 107, 108, welche den Zustand des Sicherheitsmoduls 100 signalisieren. Die Sicherheitsmodule können in ihrem Lebenszyklus verschiedene Zustände einnehmen. So muß z.B. detektiert werden, ob das Modul gültige kryptografische Schlüssel enthält. Weiterhin ist es auch wichtig zu unterscheiden, ob das Modul funktioniert oder defekt ist. Die genaue Art und Anzahl der Modulzustände ist von den realisierten Funktionen im Modul und von der Implementierung abhängig.

Anhand der Figur 5 wird das Schaltbild der Detektionseinheit 13 erläutert. Es ist vorgesehen, daß die Ungestecktsein-Detektionseinheit 13 einen Spannungsteiler aufweist, der aus einer Reihenschaltung von Widerständen 1310, 1312, 1314 besteht und zwischen einem von einem Kondensator 1371 abgreifbaren Versorgungsspannungspotential und einem Meßspannungspotential auf der Leitung 192 gelegt ist. Die Schaltung wird über die Leitung 136 mit der System- oder Batteriespannung versorgt. Die jeweilige Versorgungsspannung von der Leitung 136 gelangt über eine Diode 1369 auf den Kondensator 1371 der Schaltung. Ausgangsseitig der Schaltung liegt ein Negator 1320, 1398. Im Normalzustand ist der Transistor 1320 des Negators gesperrt und die Versorgungsspannung wird über den Widerstand 1398 auf der Leitung 139 wirksam, welche deshalb logisch '1', d.h. H-Pegel im Normalzustand führt. Ein L-Pegel auf der Leitung 139 ist vorteilhaft als Statussignal für ein Ungestecktsein, weil dann in den Pin 5 des Prozessors 120 kein Strom hineinfließt, was die Batterielebensdauer erhöht. Die Diode 1369 sorgt vorzugsweise in Zusammenhang mit einem Elektrolytkondensator 1371 dafür, daß die dem Negator vorgeschaltete Schaltung über einen relativ langen Zeitraum (> 2 s) mit einer Spannung versorgt wird, bei der deren Funktion gewährleistet ist, obwohl die Spannung auf der Leitung 136 bereits abgeschaltet wurde.

Der Spannungsteiler 1310, 1312, 1314 weist einen Abgriff 1304 auf, an welchem ein Kondensator 1306 und der nichtinvertierende Eingang eines Komparators 1300 angeschlossen sind. Der invertierende Eingang des Komparators 1300 ist mit einer Referenzspannungsquelle 1302 verbunden. Der Ausgang des Komparators 1300 ist einerseits über den Negator 1324, 1398 mit der Leitung 139 und andererseits mit dem Steuereingang eines Schaltmittels 1322 für die Selbsthaltung verbunden. Das Schaltmittel 1322 ist zum Widerstand 1310 des Spannungsteilers parallel geschaltet und das Schaltmittel 1316 für eine Rücksetzung der Selbsthaltung ist zwischen dem Abgriff 1304 und Masse geschaltet. Der Abgriff 1304 des Spannungsteilers liegt am Verbindungspunkt der Widerstände 1312 und 1314. Der zwischen dem Abgriff 1304 und Masse geschaltete Kondensator 1306 verhindert Schwingungen. Die Spannung am Abgriff 1304 des Spannungsteilers wird im Komparator 1300 mit der Referenzspannung der Quelle 1302 verglichen. Ist die zu vergleichende Spannung am Abgriff 1304 kleiner als die Referenzspannung der Quelle 1302, so bleibt der Komparatorausgang auf L-Pegel geschaltet und der Transistor

1320 des Negators ist gesperrt. Dadurch erhält die Leitung 139 nun Betriebsspannungspotential und das Statussignal führt logisch '1'. Der Spannungsteiler ist so dimensioniert, daß bei Massepotential auf der Leitung 192 der Abgriff 1304 eine Spannung führt, welche sicher unterhalb der Schaltschwelle des Komparators 1300 liegt. Wird die Verbindung unterbrochen und die Leitung 192 ist nicht mehr mit Masse verbunden, weil das Sicherheitsmodul 100 vom Sockel auf der Hauptplatine 9 bzw. Interfaceeinheit 8 der Frankiermaschine gelöst wurde, so wird die Spannung am Abgriff 1304 über die Spannung der Referenzspannungsquelle 1302 gezogen und der Komparator 1300 schaltet um. Der Komparatorausgang wird auf H-Pegel geschaltet und folglich ist der Transistor 1320 durchgeschaltet. Dadurch wird die Leitung 139 mit Massepotential verbunden und das Statussignal führt logisch '0'.

Mit Hilfe eines Transistors 1322, welcher dem Widerstand 1310 des Spannungsteilers parallelgeschaltet ist, wird eine Selbsthalteschaltung der Ungestecktsein-Detektionseinheit 13 realisiert. Der Steuereingang des Transistors 1322 wird vom Komparatorausgang auf H-Pegel geschaltet. Dadurch schaltet der Transistor 1322 durch und überbrückt den Widerstand 1310. Infolgedessen wird der Spannungsteiler nur noch durch die Widerstände 1312 und 1314 gebildet. Dadurch wird die Umschaltsschwelle so weit erhöht, daß der Komparator auch im geschalteten Zustand bleibt, wenn die Leitung 192 wieder Massepotential führt, weil das Sicherheitsmodul wieder gesteckt wurde.

Der Zustand der Schaltung kann über das Signal auf der Leitung 139 vom Prozessor 120 abgefragt werden.

Es ist vorgesehen, daß die Ungestecktsein-Detektionseinheit 13 als Schaltungsmittel eine Leitung 137 und ein Schaltmittel 1316 für eine Rücksetzung der Selbsthaltung aufweist, wobei die Rücksetzung vom Prozessor 120 über ein Signal auf der Leitung 137 auslösbar ist.

Der Prozessor 120 kann jederzeit über einen Anwenderschaltkreis ASIC 150, über eine erste Kontaktgruppe 101, über einen Systembus der Steuereinrichtung 1 und beispielsweise über den Mikroprozessor 91 per Modem 83 den Kontakt zu einer entfernten Datenzentrale aufnehmen, welche die Abrechnungsdaten überprüft und gegebenenfalls weitere Daten an den Prozessor 120 übermittelt. Der Anwenderschaltkreis ASIC 150 des Sicherheitsmoduls 100 ist mit dem Prozessor 120 über einen modulinternen Datenbus 126 verbunden.

Der Prozessor 120 kann die Ungestecktsein-Detektionseinheit zurücksetzen, wenn mittels der übermittelten Daten eine Reinitialisation erfolgreich abgeschlossen werden konnte. Dazu wird über das Rücksetzsignal auf der Leitung 137 der Transistor 1316 durchgeschaltet und somit die Spannung am Abgriff 1304 unter die Referenzspannung der Quelle 1302 gezogen und die Transistoren 1320 und 1322 sperren. Ist der Transistor 1322 im Normalzustand gesperrt, so bilden die Widerstände 1310 und 1312 in Serie den oberen Teil des oben genannten Spannungsteilers und die Umschaltsschwelle wird wieder auf den Ursprungszustand abgesenkt.

Die Figur 6 zeigt den mechanischen Aufbau des Sicherheitsmoduls in Seitenansicht. Das Sicherheitsmodul ist als Multi-Chip-Modul ausgebildet, d.h. mehrere Funktionseinheiten sind auf einer Leiterplatte 106 verschaltet. Das Sicherheitsmodul 100 ist mit einer harten Vergußmasse 105 vergossen, wobei die Batterie 134 des Sicherheitsmoduls 100 außerhalb der Vergußmasse 105 auf einer Leiterplatte 106 auswechselbar angeordnet ist. Beispielsweise ist es so mit einem Vergußmaterial 105 vergossen, daß Signalmittel 107, 108 aus dem Vergußmaterial an einer ersten Stelle herausragen und daß die Leiterplatte 106 mit der gesteckten Batterie 134 seitlich einer zweiten Stelle herausragt. Die Leiterplatte 106 hat außerdem Batteriekontaktklemmen 103 und 104 für den Anschluß der Pole der Batterie 134, vorzugsweise auf der Bestückungsseite oberhalb der Leiterplatte 106. Es ist vorgesehen, daß zum Anstecken des postalischen Sicherheitsmoduls PSM 100 auf die Hauptplatine des Meters 1 die Kontaktgruppen 101 und 102 unterhalb der Leiterplatte 106 (Leiterbahnseite) des Sicherheitsmoduls 100 angeordnet sind. Der Anwenderschaltkreis ASIC 150 steht über die erste Kontaktgruppe 101 - in nicht gezeigter Weise - mit dem Systembus einer Steuereinrichtung 1 in Kommunikationsverbindung und die zweite Kontaktgruppe 102 dient der Versorgung des Sicherheitsmoduls 100 mit der Systemspannung. Wird das Sicherheitsmodul auf die Hauptplatine gesteckt, dann ist es vorzugsweise innerhalb des Metergehäuses dergestalt angeordnet, so daß das Signalmittel 107, 108 nahe einer Öffnung 109 ist oder in diese hineinragt. Das Metergehäuse ist damit vorteilhaft so konstruiert, daß der Benutzer die Statusanzeige des Sicherheitsmoduls trotzdem von außen sehen kann. Die beiden Leuchtdioden 107 und 108 des Signalmittels werden über zwei Ausgangssignale

der I/O-Ports an den Pin 8, 9 des Prozessors 120 gesteuert. Beide Leuchtdioden sind in einem gemeinsamen Bauelementgehäuse untergebracht (Bicolorleuchtdiode), weshalb die Abmaße bzw. der Durchmesser der Öffnung relativ klein bleiben kann und in der Größenordnung des Signalmittels liegt. Prinzipiell sind drei unterschiedliche Farben darstellbar (rot, grün, orange), von denen aber nur zwei benutzt werden (rot und grün). Zur Zustandsunterscheidung werden die LED's auch blinkend benutzt, so daß 5 verschiedene Zustandsgruppen unterschieden werden können, die durch folgende LED-Zustände charakterisiert werden: LED aus, LED rot blinkend, LED rot, LED grün blinkend, LED grün.

In der Figur 7 ist eine Draufsicht auf das postalische Sicherheitsmodul dargestellt.

Die Figuren 8a bzw. 8b zeigen eine Ansicht des Sicherheitsmoduls jeweils von rechts bzw. von links. Die Lage der Kontaktgruppen 101 und 102 unterhalb der Leiterplatte 106 wird aus den Figuren 8a und 8b in Verbindung mit Figur 6 deutlich.

Erfindungsgemäß ist das postalische Gerät, insbesondere eine Frankiermaschine, jedoch kann das Sicherheitsmodul auch eine andere Bauform aufweisen, die es ermöglicht, daß es beispielsweise auf das Motherbord eines Personalcomputers gesteckt werden kann, der als PC-Frankierer einen handelsüblichen Drucker ansteuert.

Die Erfindung ist nicht auf die vorliegenden Ausführungsform beschränkt, da offensichtlich weitere andere Anordnungen bzw. Ausführungen der Erfindung entwickelt bzw. eingesetzt werden können, die - vom gleichen Grundgedanken der Erfindung ausgehend - von den anliegenden Ansprüchen umfaßt werden.

\*\*\*



### Zusammenfassung

Die Erfindung betrifft ein Verfahren zum Schutz eines Sicherheitsmoduls mit Schritten zur Überwachung des sachgemäßen Einsatzes mittels einer ersten, zweiten und dritten Funktionseinheit, Löschen von sensitiven  
5 Daten aufgrund eines unsachgemäßen Gebrauchs oder Austausches mindestens mittels der zweiten Funktionseinheit, Sperren der Funktionalität mittels der dritten Funktionseinheit während eines Austausches des Sicherheitsmoduls, Reinitialisieren der zuvor gelöschten  
10 sensitiven Daten nach sachgemäßem Gebrauch oder Austausch des Sicherheitsmoduls und Wiederinbetriebnahme durch Freischalten der Funktionseinheiten des Sicherheitsmodules. Die Anordnung zur Durchführung des Verfahrens hat eine Ungestecktsein-Detektionseinheit (13), die Schaltungsmittel (1310, 1316, 1322, 1324) für eine rücksetzbare  
15 Selbsthaltung aufweist, wobei die Selbsthaltung ausgelöst wird, wenn der Spannungspegel auf einer Meßspannungsleitung (192) von einem vorbestimmten Potential abweicht. Eine Logik umfaßt einen mit den anderen Funktionseinheiten verbundenen Prozessor (120), welcher programmiert ist, den jeweiligen Zustand des Sicherheitsmoduls (100)  
20 festzustellen und zu verändern.

Fig. 1

\*\*\*



## Ansprüche

5 1. Verfahren zum Schutz eines Sicherheitsmoduls, mit den folgenden Schritten:

- Überwachung des sachgemäßen Einsatzes mittels einer ersten, zweiten und dritten Funktionseinheit,
- 10 • Löschen von sensitiven Daten aufgrund eines unsachgemäßen Gebrauchs oder Austausches mindestens mittels der zweiten Funktionseinheit,
- Sperren der Funktionalität mittels der dritten Funktionseinheit während eines Austausches des Sicherheitsmoduls,
- 15 • Reinitialisieren mittels der ersten Funktionseinheit von zuvor gelöschten sensitiven Daten nach sachgemäßem Gebrauch oder Austausch des Sicherheitsmoduls,
- Wiederinbetriebnahme durch Freischalten der Funktionseinheiten des Sicherheitsmodules.

20 2. Verfahren, nach Anspruch 1, g e k e n n z e i c h n e t d a d u r c h, daß das Reinitialisieren in Verbindung mit einer Kommunikation mittels einer entfernten Datenzentrale von der ersten Funktionseinheit vorgenommen wird, nachdem eine dynamische Gestecktsein-Detektion erfolgreich durchgeführt wurde, wobei während der Detektion von der ersten Funktionseinheit über eine Stromschleife (18) der Interfaceeinheit (8) Informa-  
25 tionen ausgetauscht werden, deren fehlerfreie Übermittlung den Beweis für den sachgemäßen Einbau erbringt und daß das Freischalten von Funktionseinheiten (12, 13) des Sicherheitsmodules durch deren Rücksetzen erfolgt, wobei die erste Funktionseinheit ein Prozessor (120), die  
30 zweite Funktionseinheit eine Spannungsüberwachungseinheit (12) mit rücksetzbarer Selbsthaltung und die dritte Funktionseinheit eine Ungestecktsein-Detektionsschaltung (13) mit rücksetzbarer Selbsthaltung ist.

3. Anordnung zur Durchführung des Verfahrens nach Anspruch 1, wobei ein Sicherheitsmodul, mit einer Logik (120, 150, 160) und Sensoren (13), mit einer Batterie (134) und Mitteln zur Versorgung mit einer Systemspannung und mit einem Spannungumschalter (180) ausgestattet ist, der über eine Leitung (136) mit einer Spannungsüberwachungseinheit (12) verbunden ist, welche über eine Leitung (138) eine Betriebsspannung an einen Speicher (122, 124) abgibt, g e k e n n z e i c h n e t d a d u r c h, daß eine Ungestecktsein-Detektionseinheit (13) Schaltungsmittel (1310, 1316, 1322, 1324) für eine rücksetzbare Selbsthaltung aufweist, wobei die Selbsthaltung ausgelöst wird, wenn der Spannungspegel auf einer Meßspannungsleitung (192) von einem vorbestimmten Potential abweicht und daß die Logik einen mit den anderen Funktionseinheiten verbundenen Prozessor (120) umfaßt, welcher programmiert ist, den jeweiligen Zustand des Sicherheitsmoduls (100) festzustellen und zu verändern.

4. Anordnung, nach Anspruch 3, g e k e n n z e i c h n e t d a d u r c h, daß die Ungestecktsein-Detektionseinheit (13) als Schaltungsmittel eine Leitung (137) und ein Schaltmittel (1316) für eine Rücksetzung der Selbsthaltung aufweist, wobei die Rücksetzung vom Prozessor (120) über ein Signal auf der Leitung (137) auslösbar ist.

5. Anordnung, nach den Ansprüchen 3 bis 4, g e k e n n z e i c h n e t d a d u r c h, daß die Ungestecktsein-Detektionseinheit (13) einen Spannungsteiler aufweist, der aus einer Reihenschaltung von Widerständen (1310, 1312, 1314) besteht und zwischen einem von einem Kondensator (1371) abgreifbaren Versorgungsspannungspotential und einem Meßspannungspotential auf der Leitung (192) gelegt ist, wobei die Versorgungsspannung von der Leitung (136) über eine Diode (1369) auf den Kondensator (1371) gelangt, daß der Spannungsteiler (1310, 1312, 1314) einen Abgriff (1304) aufweist, an welchem ein Kondensator (1306) und der nichtinvertierende Eingang eines Komparators (1300) angeschlossen sind, daß der invertierende Eingang des Komparators (1300)

mit einer Referenzspannungsquelle (1302) verbunden ist, daß der Ausgang des Komparators (1300) einerseits über einen Negator (1324,1398) mit einer Leitung (139) und andererseits mit dem Steuereingang eines Schaltmittels (1322) für die Selbsthaltung verbunden ist, wobei das Schaltmittel (1322) zum Widerstand (1310) des Spannungsteilers parallel geschaltet ist und daß das Schaltmittel (1316) für eine Rücksetzung der Selbsthaltung zwischen dem Abgriff (1304) und Masse geschaltet ist.

10

6. Anordnung, nach Anspruch 5, gekennzeichnet dadurch, daß der Zustand der Selbsthaltung über die Leitung (139) vom Prozessor (120) des Sicherheitsmoduls (100) abfragbar ist.

15

7. Anordnung, nach Anspruch 6, gekennzeichnet dadurch, daß Meßspannungspotential auf der Leitung (192) Massepotential und das Spannungspotential auf der Leitung (139) Betriebsspannungspotential entspricht, wenn der Sicherheitsmodul (100) ordnungsgemäß gesteckt ist und daß anderenfalls auf der Leitung (139) Massepotential anliegt, wenn der Sicherheitsmodul (100) ungesteckt ist.

25

8. Anordnung, nach den Ansprüchen 3 bis 7, gekennzeichnet dadurch, daß der Prozessor (120) Speicher (122, 124) aufweist, an welche über die Leitung (138) eine Betriebsspannung  $U_{b+}$  von einer Spannungsüberwachungseinheit (12) geführt wird, daß der Prozessor (120) mit Systemspannung  $U_{s+}$  versorgt wird und einen vierten Anschluß (Pin 4) aufweist, um den Zustand der Selbsthaltung der Ungestecktsein-Detektionseinheit (13) über die Leitung (137) zurückzusetzen und einen fünften Anschluß (Pin 5) aufweist, an welchem die Leitung (139) angeschlossen ist, um den Zustand der Ungestecktsein-Detektionseinheit (13) abzufragen.

30

9. Anordnung, nach Anspruch 8, g e k e n n z e i c h n e t d a d u r c h, daß das Sicherheitsmodul (100) einen Anwenderschaltkreis ASIC (150) aufweist und daß der Prozessor (120) über einen modulinternen Datenbus (126) mit dem Anwenderschaltkreis ASIC (150) verbunden ist, wobei letzterer über eine erste Kontaktgruppe (101) mit dem Systembus einer Steuereinrichtung (1) in Kommunikationsverbindung steht.

10. Anordnung, nach einem der Ansprüche 3 bis 9, g e k e n n z e i c h n e t d a d u r c h, daß das Sicherheitsmodul (100) mit einer harten Vergußmasse (105) vergossen ist, daß die Batterie (134) des Sicherheitsmoduls (100) außerhalb der Vergußmasse (105) auf einer Leiterplatte (106) auswechselbar angeordnet ist, daß die Leiterplatte (106) die Batteriekontaktklemmen (103 und 104) für den Anschluß der Pole der Batterie (134) und eine zweite Kontaktgruppe (102) zur Versorgung des Sicherheitsmoduls (100) mit der Systemspannung aufweist und daß mindestens eine der Kontaktgruppen (101, 102) zur statischen und dynamischen Überwachung des Angestecktseins des Sicherheitsmoduls (100) ausgebildet ist.

20

11. Anordnung, nach Anspruch 10, g e k e n n z e i c h n e t d a d u r c h, daß der Prozessor (120) Anschlüsse (Pin's 6, 7) zur dynamischen Überwachung des Angestecktseins des Sicherheitsmoduls aufweist, an welcher Leitungen angeschlossen sind, welche zu einer Stromschleife (18) verbunden sind, wenn das Sicherheitsmodul (100) gesteckt ist.

25

12. Anordnung, nach einem der Ansprüche 3 bis 11, g e k e n n z e i c h n e t d a d u r c h, daß der Prozessor (120) des Sicherheitsmoduls (100) mit Anschlüssen (Pin's 8, 9) zur Ausgabe mindestens eines Signals zur

30

Signalisierung des Zustandes des Sicherheitsmoduls (100) ausgestattet ist.

- 5      13. Anordnung, nach Anspruch 12, gekennzeichnet dadurch, daß an den I/O-Ports einer Ein/Ausgabe-Einheit (125) des Prozessors (120) modulinterne Signalmittel (107,108) angeschlossen sind.

10

\*\*\*\*\*

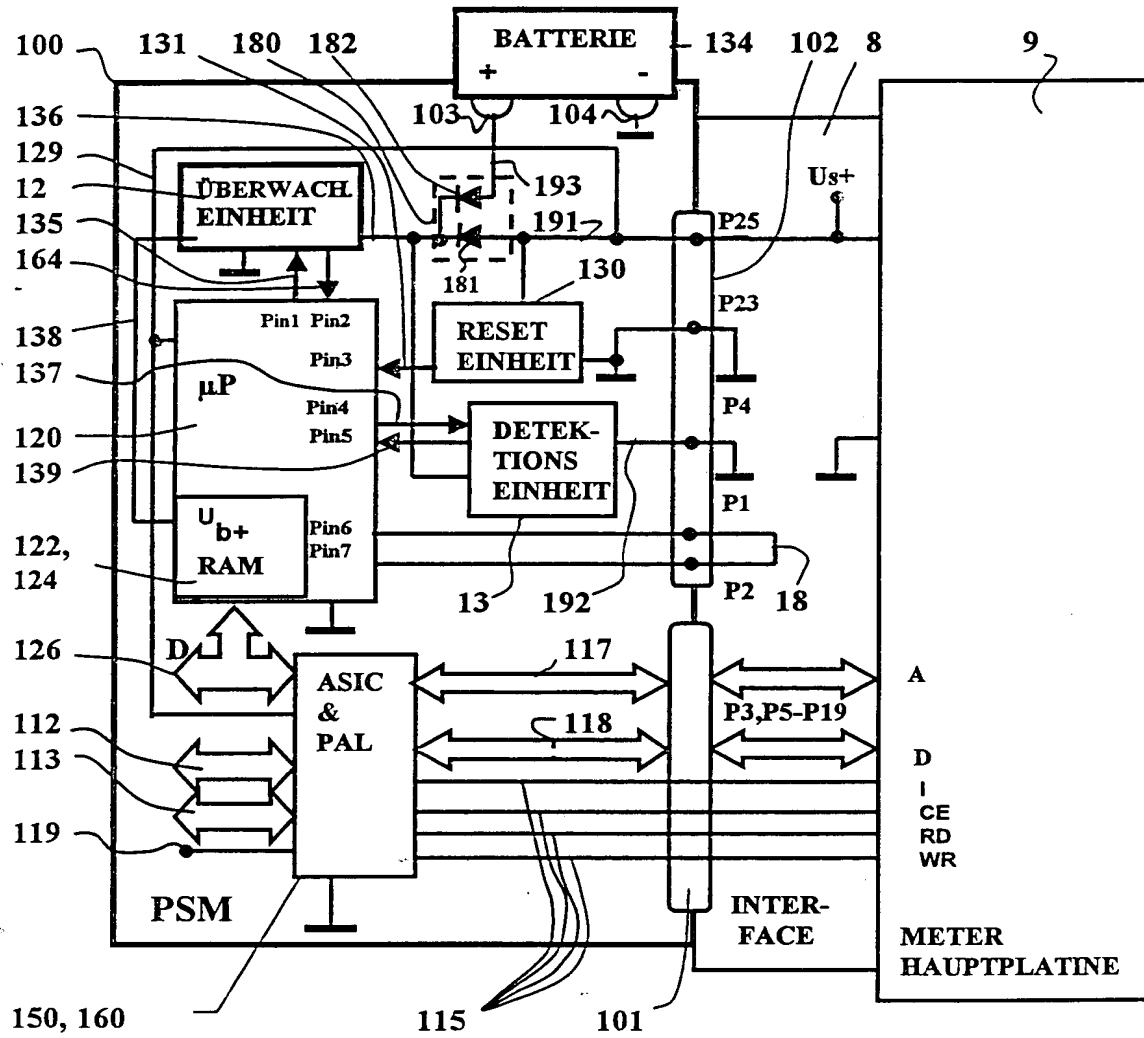


Fig. 1



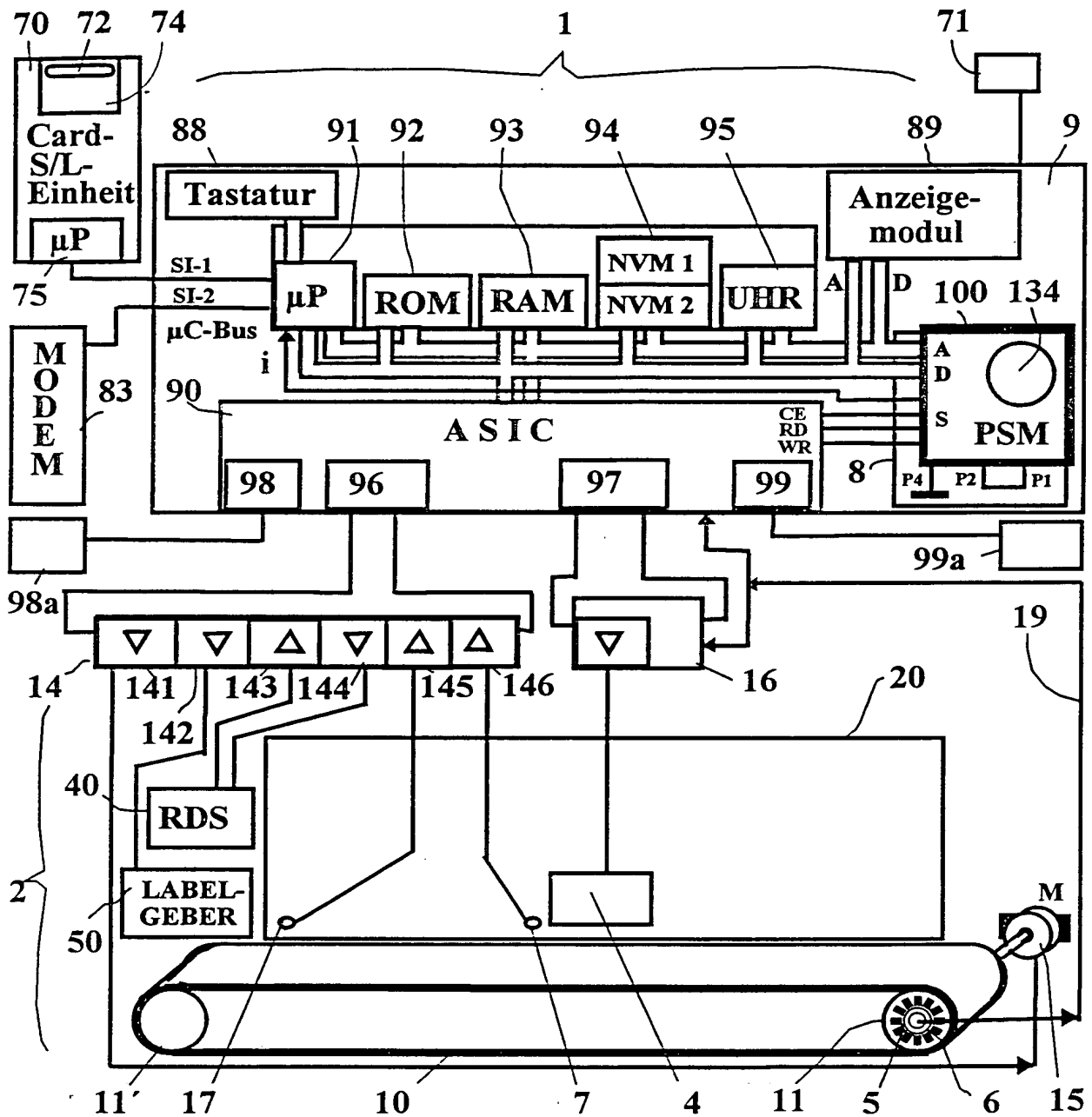


Fig. 2

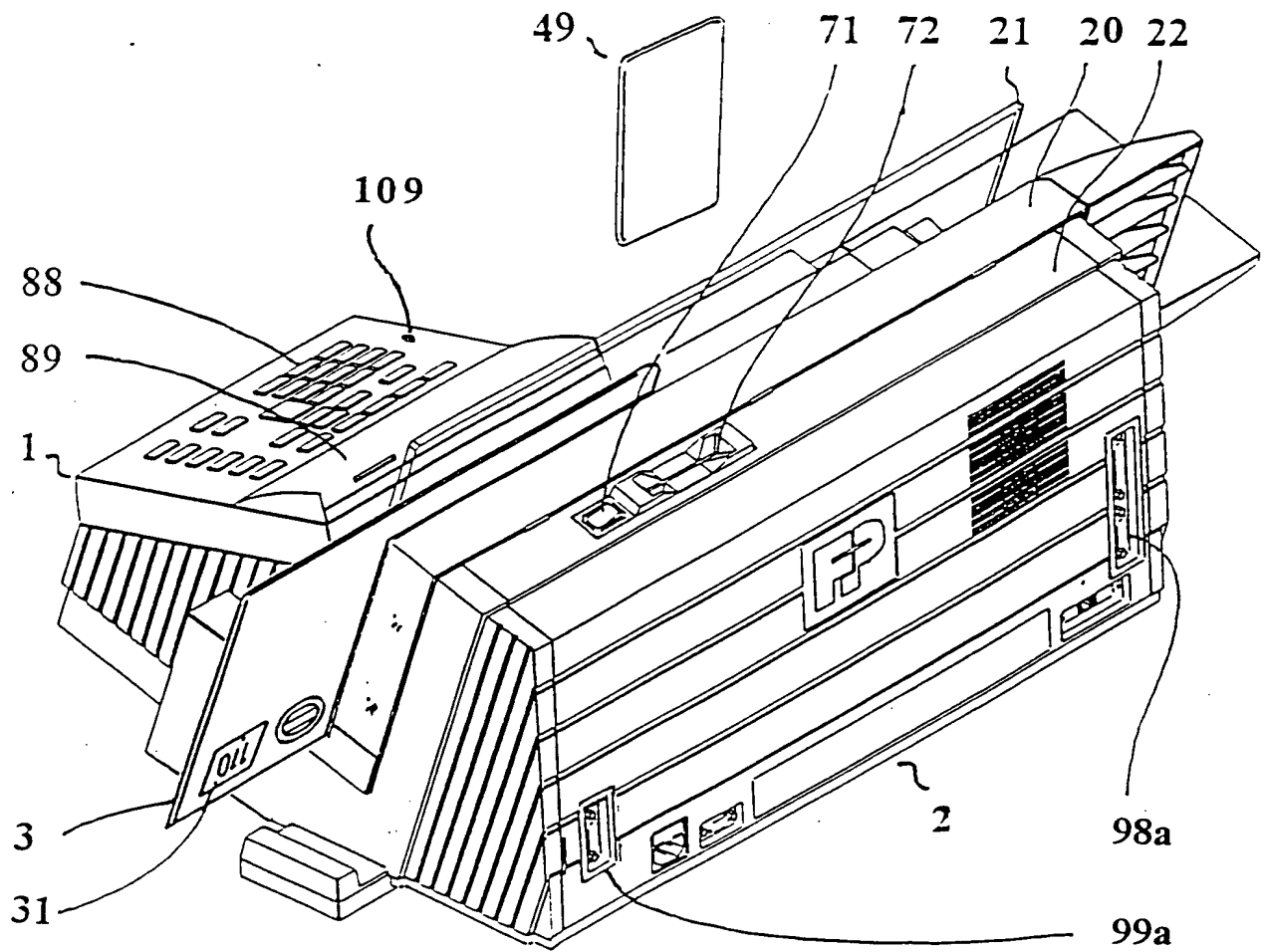


Fig. 3

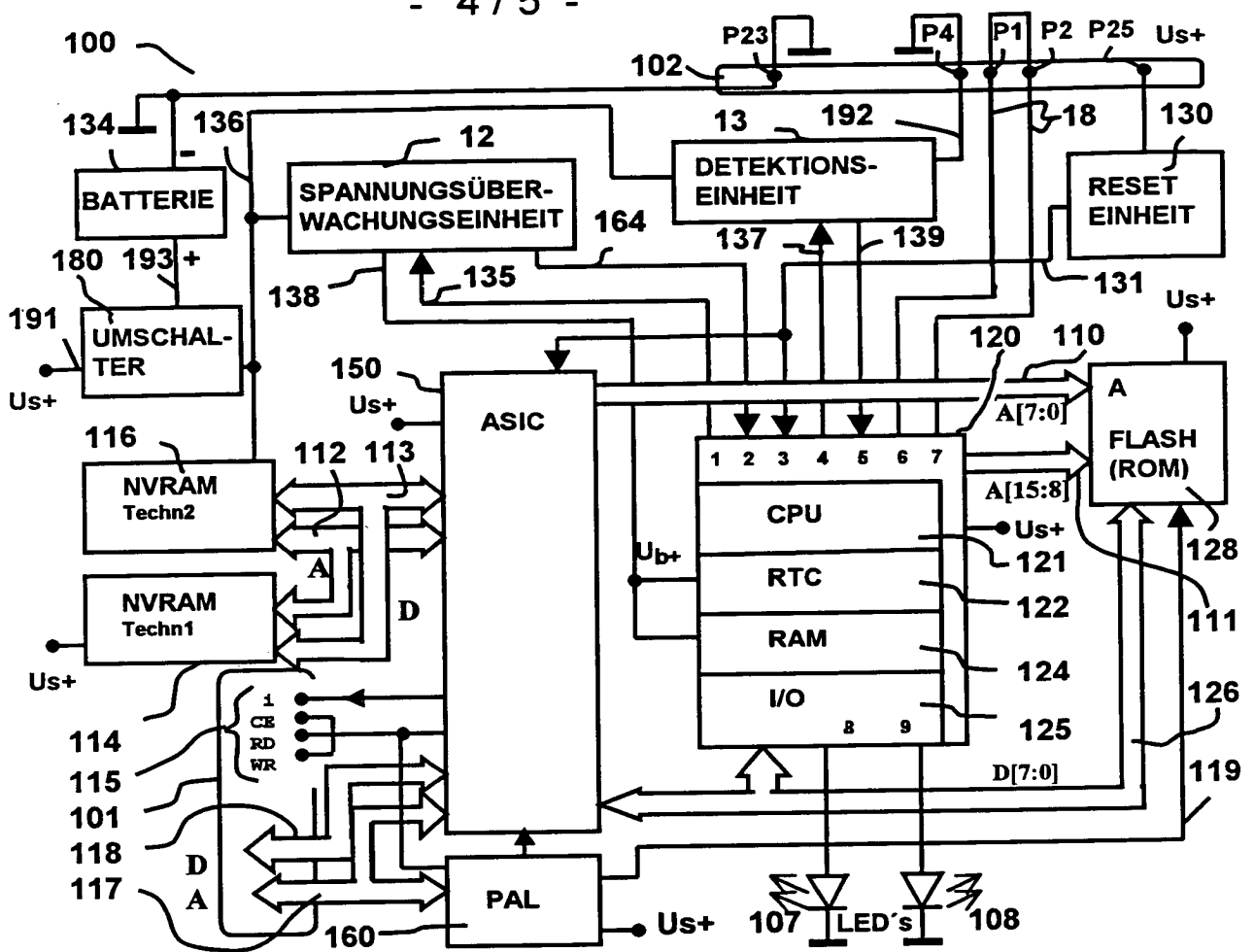


Fig. 4

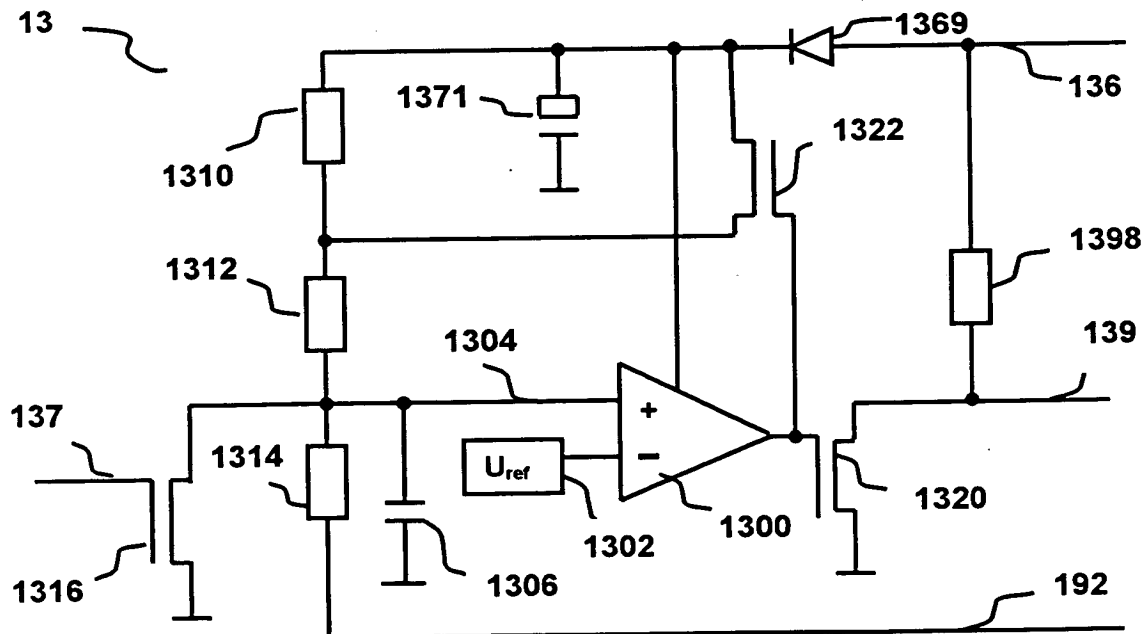


Fig. 5

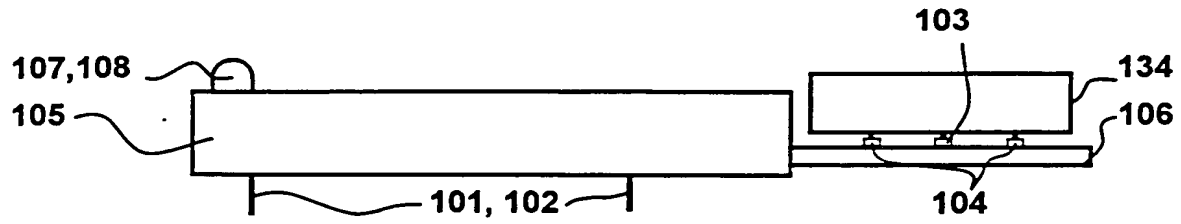


Fig. 6

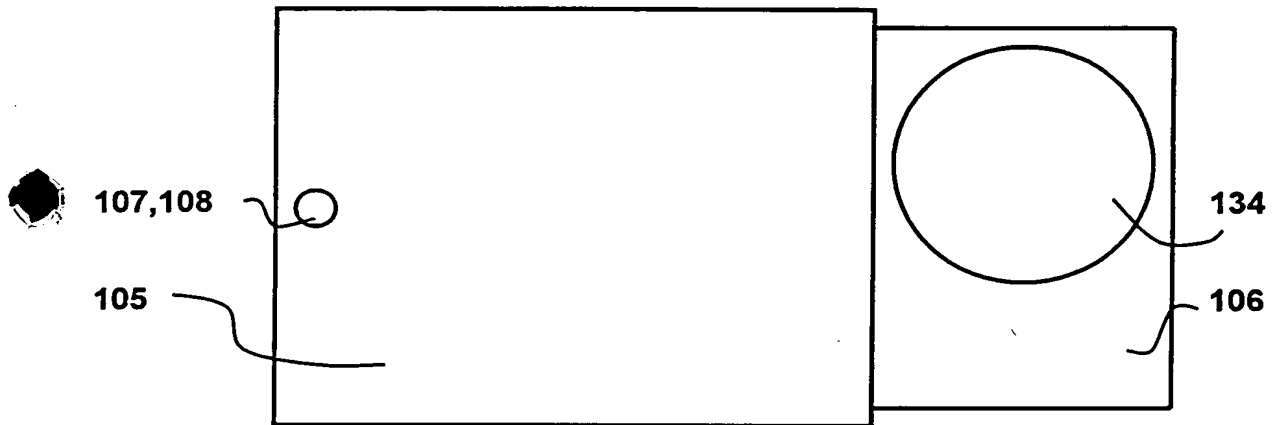


Fig. 7

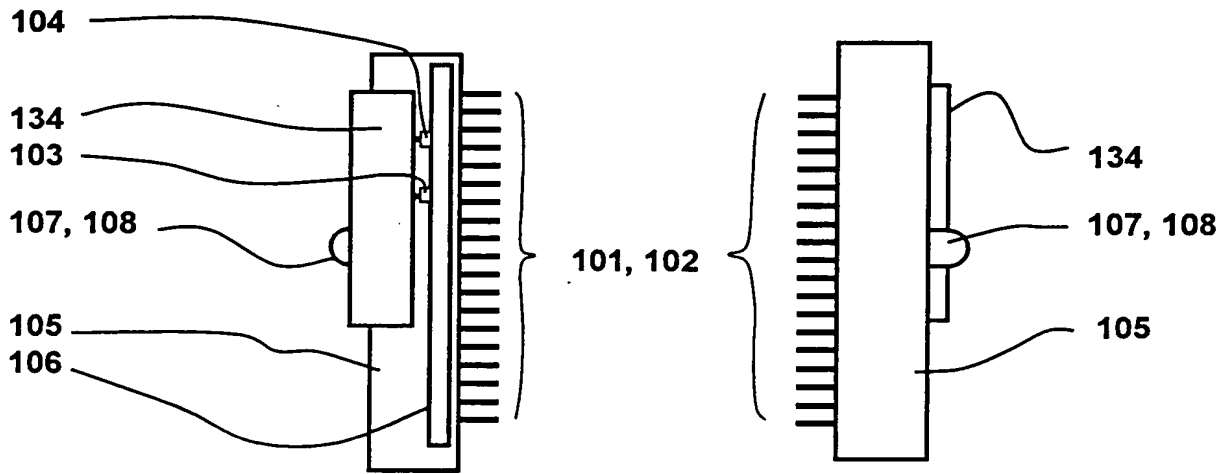


Fig. 8a

Fig. 8b